A CASTAWAY'S GUIDE TO THREAT INTELLIGENCE AND INFORMATION SHARING

DIR INFORMATION SECURITY FORUM - APRIL 14, 2016

BRIAN A. ENGLE – EXECUTIVE DIRECTOR

R-CISC
RETAIL CYBER INTELLIGENCE SHARING CENTER

R-CISC.org ©2016

AGENDA

Information Sharing

- Information Sharing is Only for the Advanced
- Not the Solution to the Problem

Threat Intelligence

- There Is a Magic Source of Context
- Actionable Automation: Fire – Ready – Aim

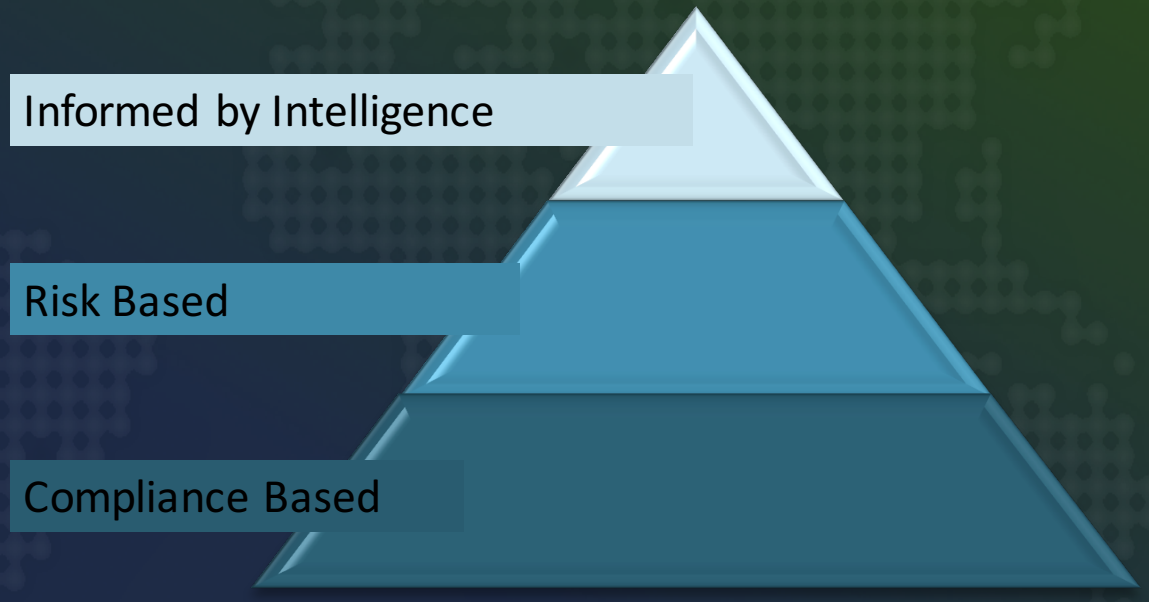
R-CISC.org ©2016

INFORMATION SHARING

R-CISC.org ©2016

EVOLUTION AND THE HIERARCHY OF NEEDS

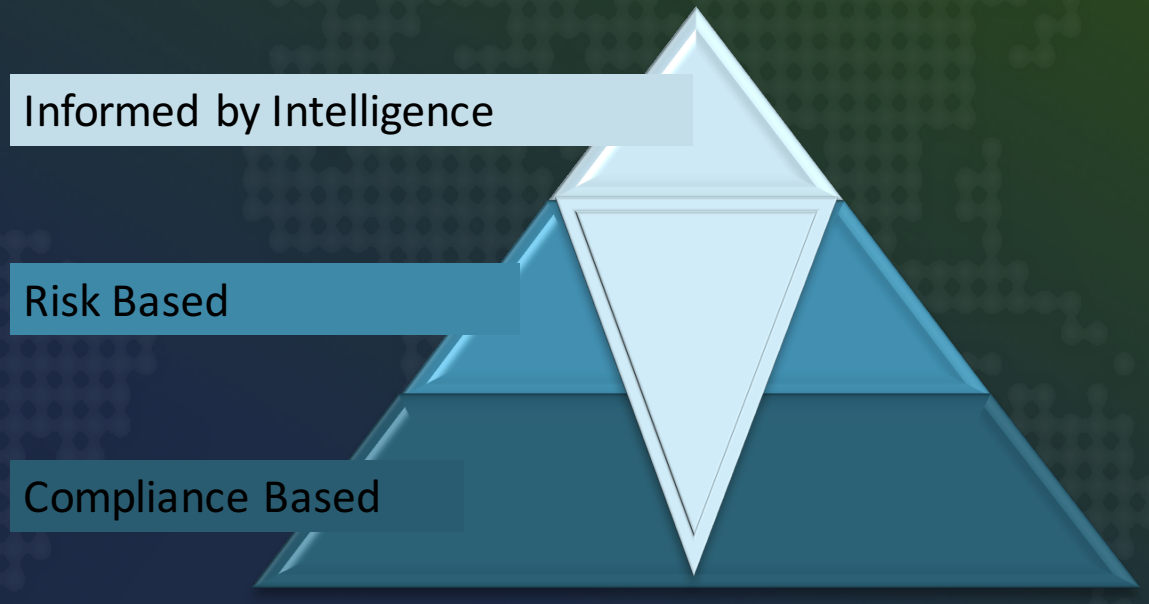
Sharing is Needed to Build Capability, But Many Wait to Be '**Ready**' to Share



R-CISC.org ©2016

EVOLUTION AND THE HIERARCHY OF NEEDS

Information Sharing is Fundamental and Essential, Not Aspirational



BENCHMARKING:
GOING BEYOND KEEPING UP WITH THE JONESES

Overwhelmed about where to start…

…or underwhelmed by the information available.

STATE OF TEXAS CYBERSECURITY FRAMEWORK

Functions

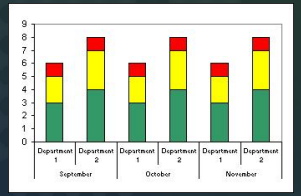
- IDENTIFY
- PROTECT
- DETECT
- RESPOND
- RECOVER

OBJECTIVES

CONTROLS

COMPARISON OPPORTUNITIES

Investment needed and Costs to operate



Progress to roadmap goals

Best practices for improving

LEARNING FROM THE (MIS)FORTUNE OF OTHERS

Cheat – Copy liberally from others

Consider as many external input and output process opportunities as possible…

…to see around the corners.

Find a tribe, then share tribal knowledge

INFORMATION SHARING DOESN'T WORK?!

VISIBILITY -- CLARITY -- INFORMATION

THREAT INTELLIGENCE

R-CISC.org ©2016

THREAT INTELLIGENCE FEEDS – INTEL AS A SERVICE

Doing the dirty work that you can't or don't want to do

SET MY INTEL FREE

The Threat Intel Hostage Situation

Did you know you're already sharing?

"I WANT MY THREAT INTEL TO BE ACTIONABLE"

BAKING THE CONTEXT INTO THE INTEL

What defines relevancy for *you*?

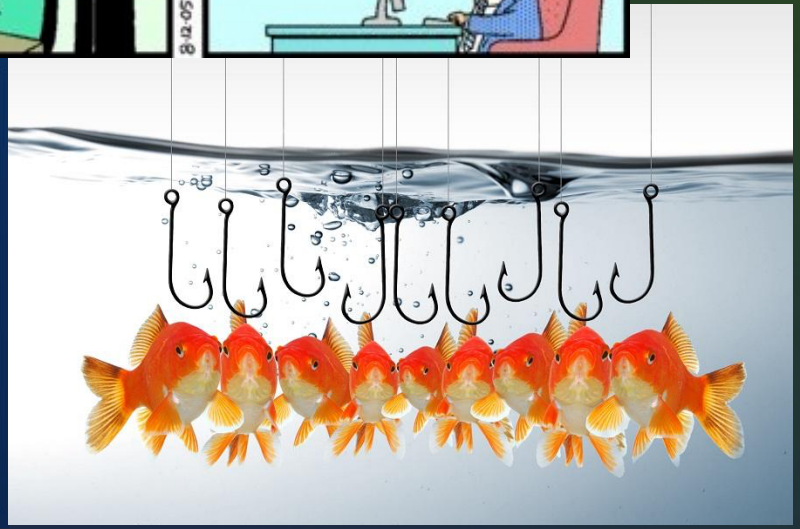
What defines significance, and how is it prioritized?

Target of opportunity, or singled out?

What makes intelligence reliable? Trustworthy?

Are you willing to wait for perfect intel, or is good enough good enough?

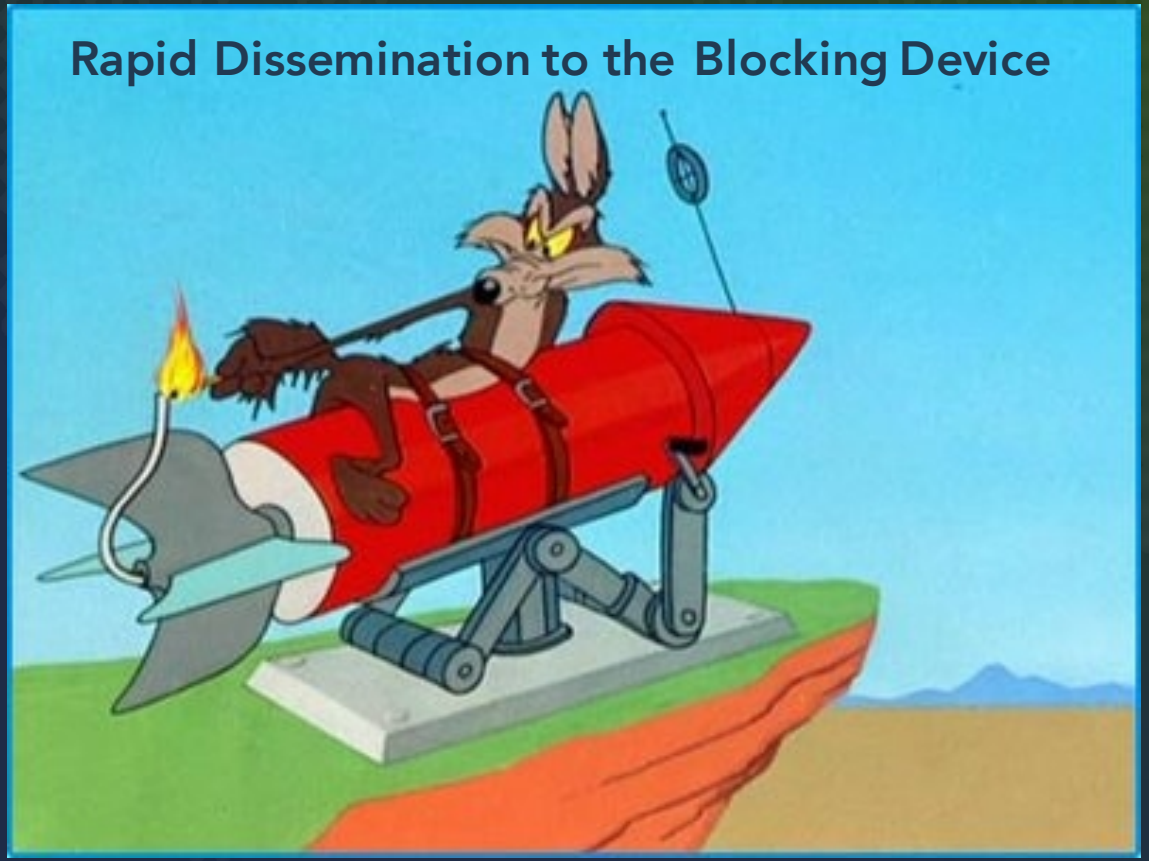
COLLECTIVE INTELLIGENCE



AUTOMATING THREAT INTELLIGENCE

R-CISC.org ©2016

FIRE, READY, AIM



AUTOMATION WITHIN THE INTELLIGENCE PROCESS

Collection

- Process x000's of indicators/sources/observations
- Wheat v. Chaff

Production

- Homer's "Odyssey" on an Etch a Sketch

Dissemination

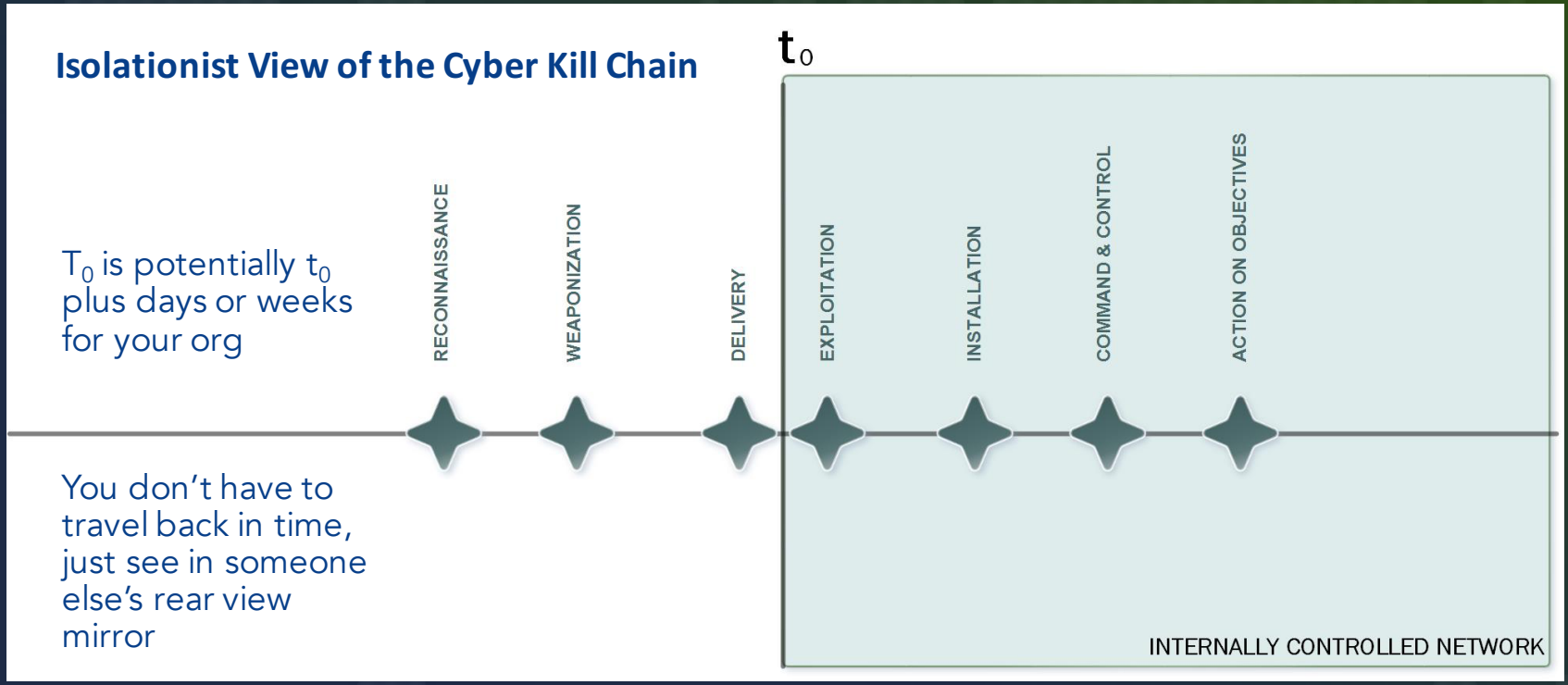
- Let's schedule a conference room and have a meeting

Feedback

- Advancing the "Context" issue with less effort

MAGNIFY YOUR THREAT INTEL

KILL CHAIN AND THE POINT OF IMPACT



HUNTING AND THE KILL CHAIN

How many alerts per day can your team process?

- Consider 15 minutes per alert per analyst
- 32 per FTE per shift

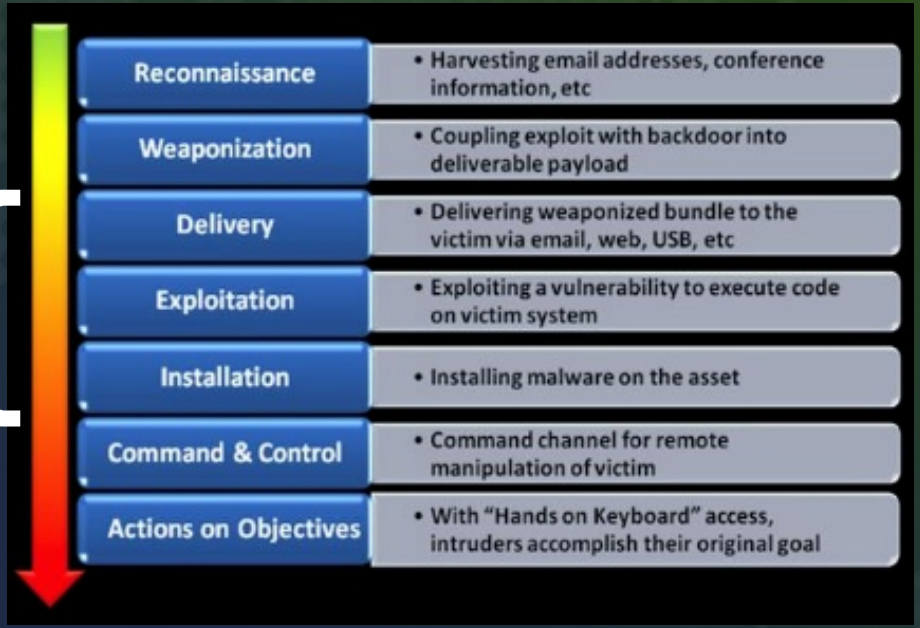
Where are your analysts able to spend their time hunting?

- Can they afford to be curious?

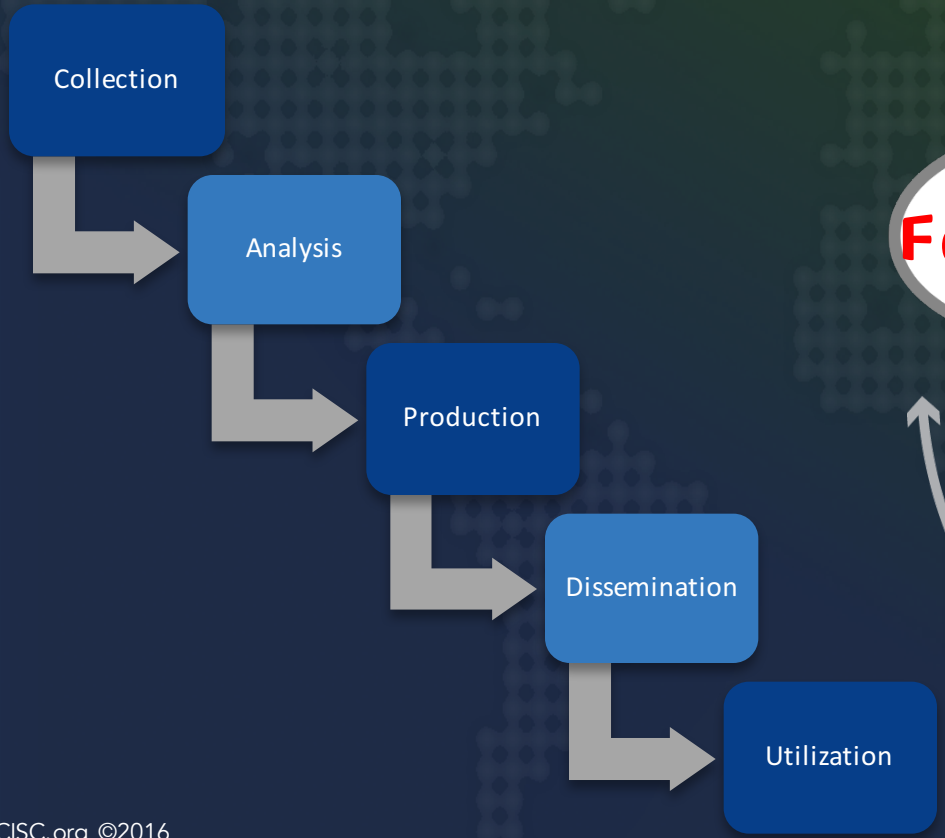
Point of impact

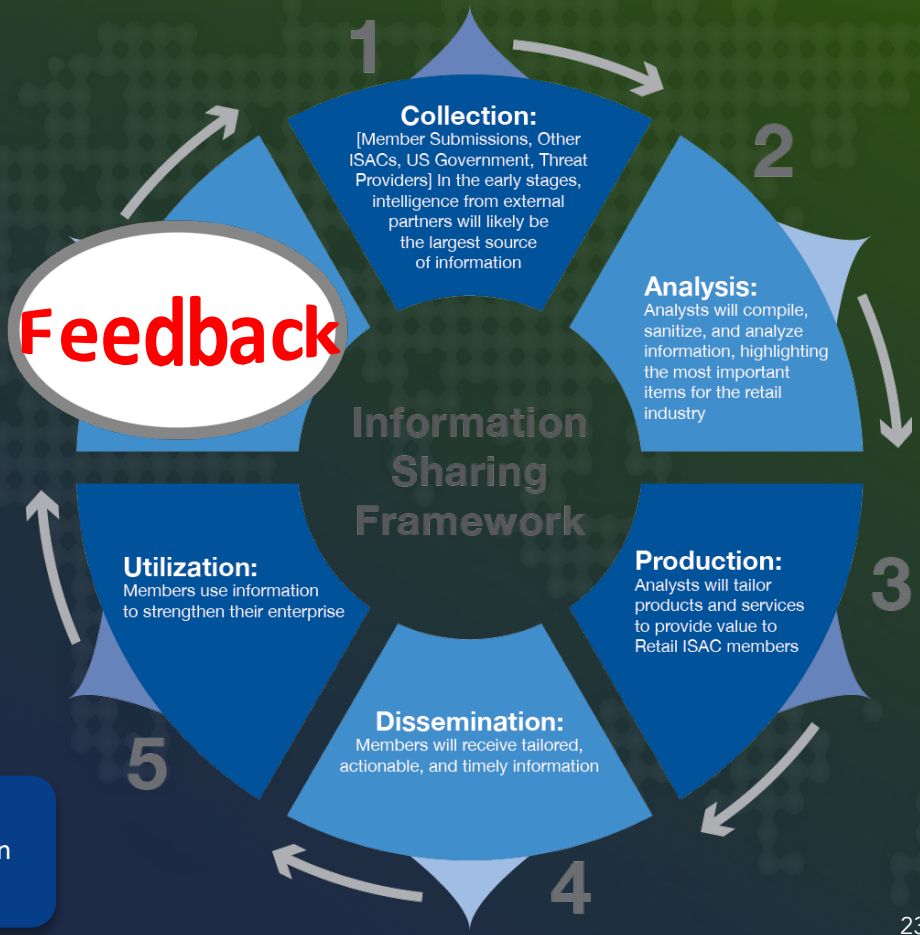
Before impact, intelligence you need gathered

After impact, need to be actively hunting



INTELLIGENCE FEEDBACK – THE CONTEXT ENGINE





GETTING OF THE ISLAND

R-CISC.org ©2016

THE BUSINESS CASE - STRATEGIC DECISION SUPPORT

Reinventing the wheel

Limiting uncertainty and identifying risk

Rigidly banging away at yesterday's problem


ISLANDS

ABOUT THE R-CISC

The Retail Cyber Intelligence Sharing Center (R-CISC) is the **trusted** cybersecurity resource for all retailers, commercial services entities, and cyber security industry partners worldwide.

Created in response to the increased number and sophistication of attacks against our industries, the R-CISC provides the **community** of organizations **serving** consumers with apparel, food, lodging, entertainment and other forms of commercial services a significant tool to combat cyber criminals by **sharing** leading practices and threat intelligence within in a safe and secure way.

Through an integrated community of **cooperating** organizations, we are **stronger together**.

R-CISC.org ©2016

CONTACT THE R-CISC

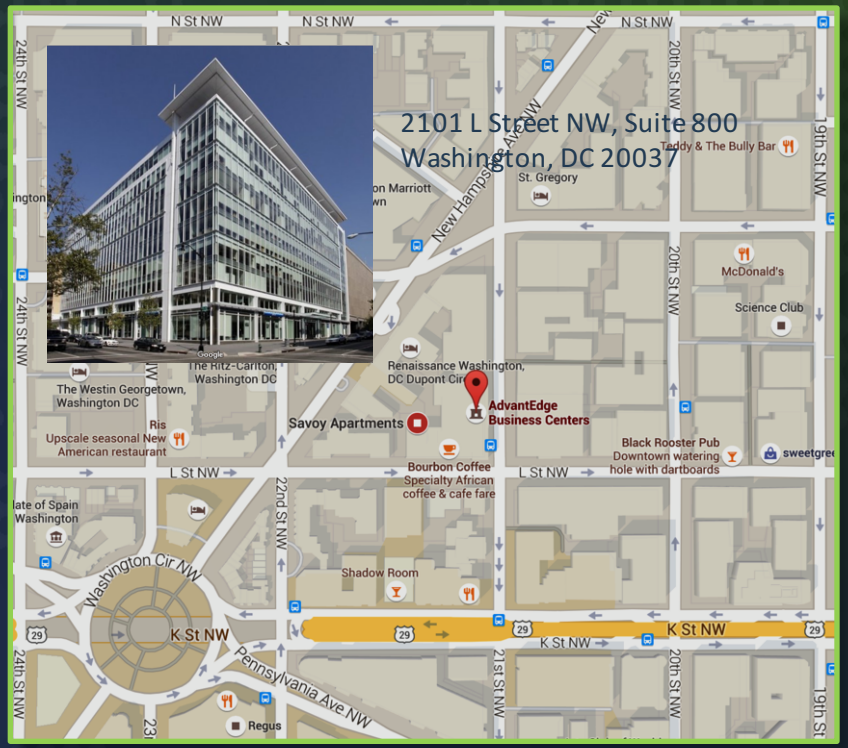
membership@r-cisc.org

info@r-cisc.org

www.r-cisc.org

@retailcisc

(202) 466-0538



Brian.engle@r-cisc.org

@brianaengle